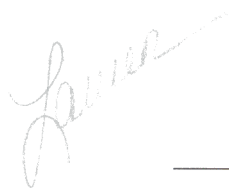


4100 E. Milham Avenue
Kalamazoo, MI 49001

t: 269 323 7700 800 253 3210
www.stryker.com



stryker®

Instruments

April 10, 2008

Kelly A. Ayotte
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Breach

To Whom it May Concern:

The purpose of this letter is to inform you of a security breach that potentially involves confidential, personal information regarding certain residents of your state.

On February 18, 2008, Stryker Instruments, a division of Stryker Corporation (collectively, "Stryker"), discovered that an unauthorized user recently gained access to its virtual private network (VPN) multiple times over a period of several months. Stryker immediately disabled the domain administrator service account through which the unauthorized user had accessed the VPN. It then promptly began investigating the incident and engaged an independent computer forensics investigator to determine the scope of the breach and the identity of the unauthorized user.

The investigation revealed that the unauthorized user accessed several Stryker servers and applications. One of the servers accessed by the unauthorized user contained a database of Social Security numbers of certain employees in 48 different states and Puerto Rico. Stryker and its computer forensics investigator were unable to conclude whether the database was actually accessed or whether any Social Security numbers were acquired.

Based on the manner in which the user acquired access to Stryker's network and the user's network activity, Stryker believes the unauthorized user is a former employee with prior knowledge of the network. Stryker suspects a particular former employee, but has been unable to confirm whether that individual is, in fact, the unauthorized user.

On March 4, 2008, Stryker contacted the office of its local U.S. Attorney and the Federal Bureau of Investigation in Kalamazoo, Michigan to inquire whether the FBI would investigate the matter further. Since then, Stryker has been engaged in informal discussions with the FBI about a potential criminal investigation. Initially, the FBI asked Stryker not to give notice of the security incident, so as not to interfere with its investigation. But on March 20, 2008, the FBI informed Stryker that based on current information, it would not pursue a criminal investigation.

At this time, Stryker has not been able to confirm that any Social Security numbers or other personal employee information was accessed. Because it cannot rule out the possibility that Social Security numbers were accessed or acquired, however, Stryker will provide a notice of the security incident to each potentially affected employee. Stryker intends that the notices will comply with the state security breach notification laws in each state whose residents were potentially affected. The number of residents of your state who are potentially affected is seven.

Stryker intends to mail the notice to affected employees on April 10, 2008. A sample copy of the notice that will be provided to residents of your state is attached with this correspondence.

In order to prevent future security breaches of this nature, Stryker took certain action immediately after discovering this breach. Stryker has discontinued access to the VPN through the domain administrator service accounts. It also performed an audit of its privileged access accounts and eliminated any unnecessary service accounts. Further, it changed the passwords of all service accounts. Stryker has also implemented a policy to prohibit user password changes via telephone.

Stryker also plans to implement a number of additional preventative measures in the coming months. These measures include:

- Developing procedures to ensure that access to Stryker's network will be disabled immediately upon an employee's termination;
- Developing a procedure to review service accounts and change passwords;
- Eliminating potential gaps in Stryker's current internal audit system;
- Requiring two-factor authentication for all remote network access;
- Disabling one of Stryker's existing VPNs and moving all users to a single, more secure VPN; and
- Implementing a system of consolidating and monitoring user log files for potential security breaches.

If you have any questions or would like additional information about the security incident, the results of Stryker's investigation, its notice to affected employees or its actions to prevent future security breaches, please call ID TheftSmart member services at 1-800-588-9839 between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday.

Sincerely,



Jud Hoff, Vice President
Compliance Officer



Curt Hartman, President
Global Instruments

Enclosure- Copy of Notice to Residents of Security Breach



Secure Processing Center | PO Box 37420 | Oak Park, MI 48237

Urgent Message from Stryker Instruments.
Please Open Immediately.

<FirstName> <MiddleInitial> <LastName> <Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City> <State> <Zip>
<POSTNET BARCODE>

Dear <FirstName> <MiddleInitial> <LastName> <Suffix>,

We are writing to inform you of an event that may affect you. Regrettably, on February 18, 2008, Stryker Instruments ("Stryker"), through its normal network system management, discovered that an unauthorized user gained access to some of its computer systems. Through our immediate investigation, we have determined that one of the locations accessed by the unauthorized user was a server, which contained a database of Social Security numbers of certain current, former, and contracted temporary employees. Your name and Social Security number were in that database.

At this time, we cannot confirm whether the unauthorized user accessed or acquired any Social Security numbers. Although we have no reason to believe that the unauthorized user was targeting Social Security numbers, we want to make you aware of the incident and the steps we have taken to guard against identity fraud. Stryker, together with an independent computer forensics investigator, has, and continues to aggressively investigate the incident. Appropriate law enforcement agencies have also been notified. Immediately after the breach was discovered, we disabled the account that the unauthorized user used to gain access to Stryker's network, changed passwords of certain user accounts, and implemented a new, more secure password change policy. Our pledge is to continue to investigate to the fullest extent possible to determine the identity of the user and what information, if any, was compromised in this unauthorized access. Stryker also plans to implement a number of additional security measures in the coming months to prevent future security breaches.

We have also engaged Kroll Inc., the world's leading risk consulting company, to provide you with access to its ID TheftSmart™ service. This service includes Enhanced Identity Theft Restoration and Continuous Credit Monitoring, all at no cost to you.

ID TheftSmart is one of the most comprehensive programs available to help protect your name and credit against identity theft. We urge you to read the enclosed information about the safeguards now available to you.

To further safeguard yourself against identity theft or other unauthorized use of personal information, you can take some simple steps. You should remain vigilant for incidents of identity fraud and closely monitor your bills, financial accounts and free credit reports. You should also promptly report any suspected identity theft or fraud to your local law enforcement agency, the U.S. Federal Trade Commission, your financial institution, and one of the three national consumer reporting agencies listed below.

TransUnion
Consumer Relations &
Fraud Assistance
1561 E. Orangethorpe Ave.
Fullerton, CA 92831
1-800-372-8391
www.transunion.com

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian
Consumer Fraud Assistance
P.O. Box 9556
Allen, TX 7501
1-888-397-3742
www.experian.com

If you have any questions or believe you may have an identity theft issue, please call ID TheftSmart member services at 1-800-588-9839 between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday.

In closing, we apologize for this incident and any inconvenience it may cause. You have our pledge that we will do everything possible to ensure the security and protection of all personal information.

Sincerely,



Jud Hoff, Vice President
Compliance Officer



Curt Hartman, President
Global Instruments

ID TheftSmart™

<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday
If you have questions or feel you may have an identity theft
issue, please call ID TheftSmart member services

ID TheftSmart™

<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday
If you have questions or feel you may have an identity theft
issue, please call ID TheftSmart member services

Please detach cards and keep in a convenient place for your reference